Response to NCUA Request for Information and Comment on Digital Assets and Related Technologies

Submitted By:

Accenture Federal Services LLC (Accenture)
800 N. Glebe Road, Suite 300
Arlington, VA 22203

Point of Contact:

Allison J. Turner
Contract Manager
allison.j.turner@accenturefederal.com
(571) 414 - 4714

Contents

Introduction

Accenture Federal Services (AFS) is submitting this document in response to the National Credit Union Administration's (NCUA) request for information and comment on digital assets and related technologies. We commend NCUA for engaging with the industry during this critical time where rapid innovation is spurring adoption and garnering heightened regulatory attention. Our response is informed by the primary experience areas AFS has with other U.S. Federal financial regulators and agencies. This experience spans across digital asset related IT infrastructure, blockchain analytics, and advisory services.[1]

Digital asset innovation has created new markets and is disrupting the financial services industry. Some of the key issues financial regulators are facing with the digital asset industry in the United States include:

- Lack of transparency
- Threat of market manipulation
- Complexity of underlying technologies
- Rapid pace of industry development

Assisting our financial regulatory clients in responding to these and other challenges they face is critical to establishing the United States as a global leader in this growing sector of finance. Our current view of the digital asset industry, illustrated in Figure 1, is divided into two main areas: assets/infrastructure and supporting services. Considering the rapid evolution of the industry and its increasing impact to financial services, it is important for NCUA to maintain a holistic awareness of the digital asset industry.

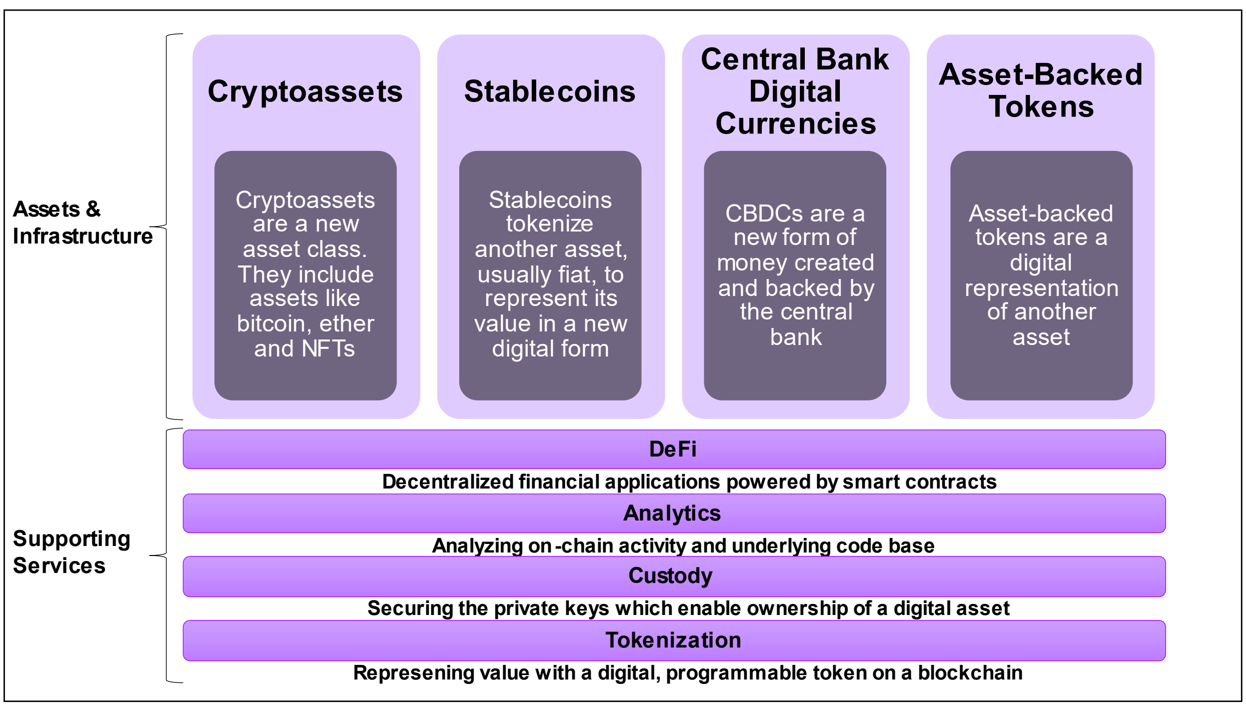

Figure 1 – Current State Overview of Digital Assets, Infrastructure and Supporting Services

[1] https://www.accenture.com/us-en/insights/us-federal-government/future-digital-currency

AFS approaches digital assets as an opportunity for a more efficient, resilient, transparent, and inclusive financial system. Regulators, such as the NCUA, can enable these benefits by providing clear guidance and rules for entrepreneurs and innovative companies to deliver value through new digital asset products and services.

The innovation coming from the digital asset industry must be balanced with the appropriate amount of education, consumer protection, anti-money laundering (AML/BSA), supervision, and monitoring activities. Regulators have the responsibility to produce reasonable frameworks which mitigate bad actors from using digital assets and underlying technologies for nefarious purposes.

Due to the various services federally insured credit unions (FICUs) provide to the American public, NCUA must have a comprehensive approach to digital assets. Cryptoassets provide the public new markets and asset classes to potentially generate wealth. Stablecoins and CBDC promise to be the new digital payment rails commerce is transacted upon. Asset-backed tokens could enable new transparency and greater access to market participants.

Making these assets usable in decentralized applications (DApps) is decentralized finance (DeFi). DeFi has shown the primitives of a new financial services system built on-chain (on top of DLT and blockchains) to facilitate exchanges, borrowing and lending, savings, wealth management and other services in an automated manner. In just a few years, DeFi DApps have attracted close to $100B, measured in total value locked (TVL), in funds across different use cases. [2] With this rapid growth has come fraud and opportunists, using false labeling to take advantage of market participants with decentralized in name only or “DINO” applications which can present risks and fraudulent claims to users and investors.

The NCUA must strive to deeply understand both the benefits and risk of digital assets, DeFi and other related technologies by conducting market research, technical deep dives and hands-on learning when possible. These actions will enable NCUA to confidently provide guidance and rulemaking for FICUs to engage with digital asset and DeFi innovation.

Responses to Questions

In response to NCUA’s request about DLT and DeFi, we have structured feedback around the areas of Operations, Risk and Compliance Management; Supervision and Activities; Share Insurance and Resolution; and Additional Considerations. Our feedback includes recommendations and key concepts for NCUA’s consideration featured throughout our response as call out boxes on the right-hand side of the page.

Operational Questions (#9)

9. How dependent will FICUs be on third-party software and open-source libraries for their own DLT projects?

FICUs will have the freedom of choice to decide how dependent they want to be on third-party software and open-source libraries for DLT projects. There are numerous examples of both private, in-house development of DLT code and open-source use by enterprises. Various

[2] https://defipulse.com/

companies, such as JPMorgan, have leveraged open-source libraries and then customized the protocols with specific parameters to suit their needs.[3]

FICUs should leverage and embrace the open-source nature of DLT and DeFi projects when feasible. Due to the large and growing community of developers contributing to the open-source libraries for DLT and digital asset projects, it is likely most efficient for FICUs to stand on the shoulders of this work by the industry. This open-source development has already produced numerous technical standards which FICUs should become familiar with, such as the ERC20 (fungible) and ERC721 (non-fungible) token standards and DeFi technologies such as Pair smart contracts. Additionally, FICUs should prioritize technology interoperability and consider how to engage with a future where multiple DLT and/or blockchains must interact with each other for various use cases.

All third-party software and open-source libraries should be considered with respective risks to use, included but not limited to the developer community ceasing to support and/or new features which have not been battle tested in a live production environment.

Risk and Compliance Management Questions (#10-11, 13-15, 17)

10. To what extent are existing risk and compliance management frameworks designed to identify, measure, monitor, and control risks associated with various DLT and DeFi applications? Do some DLT and DeFi applications more easily align with existing risk and compliance management frameworks compared to others? Do, or would, some DLT and DeFi applications result in FICUs developing entirely new or materially different risk and compliance management frameworks?

Certain DLT and DeFi use cases could require new or materially different risk and compliance frameworks. Different digital asset use cases will require different underlying blockchains or DLTs. These different blockchain and DLT systems have different underlying design patterns, standards and interfaces, make tradeoffs to optimize for certain use cases, and have different environmental, social and governance (ESG) profiles. It is possible that FICUs could adopt current risk and compliance (i.e., AML/BSA) standards, then add new standards for operational, technological and other nuanced risk considerations specific to digital assets use cases.

Use cases which include the use of permissionless blockchain networks (i.e., Bitcoin, Ethereum) require frameworks for the operational and technological risks of a global, open source network, which is maintained by distributed developers and secured by distributed miners/validators. Because these permissionless networks' actors are not all known, FICUs should prioritize fraud mitigation in their risk frameworks. Appropriate cybersecurity is required for the custody of private keys, which enable ownership of assets. Depending on the design and deployment patterns of digital assets, if the private keys of certain assets are compromised or lost, then these assets could be stolen or rendered permanently inaccessible. Furthermore, risks around enterprise data security, including information leakage linking customers and their financial activity, should be included in risk and compliance management frameworks.

Use cases which include permissioned blockchain and DLT networks require appropriate cybersecurity controls at both the private key custody level and the underlying node environment. Because permissioned networks assume that all actors participating in a network are known and

[3] https://www.jpmorgan.com/solutions/cib/news/jpmorgan-and-microsoft-announce-strategic-partnership-to-drive-enterprise-adoption-of-quorum

approved by other members, a heavy trust reliance is made on identity and membership service providers that could result in external provider risks. Fundamentally, these permissioned networks tend to have different risk profiles than permissionless networks, therefore, regulatory frameworks should be designed with these differences in mind. A high level comparison between permissionless and permissioned networks can be seen in Figure 2 below:

Permissionless	Permissioned
• **Anyone can have access to the underlying data and transaction history.** • **All participants in the network are treated as equal, meaning that all users have equal rights to read data and execute transactions.** • **They are frictionless for anyone to transact on and provide everyone the ability to access a complete copy of the transaction history.**	• **One or more organizations control who can have access to the underlying data and transaction history.** • **User identities are authenticated and known through some type of procedure (e.g. KYC/AML).** • **Different levels of read and write access can be assigned to participants for various types of data in the distributed ledger. This enables greater control and privacy than permissionless blockchains.**

Figure 2 – Regulatory frameworks should consider the differences across networks

It should be of note that permissionless and permissioned networks are not necessarily mutually exclusive and that design patterns could follow a hybrid approach in which certain activities are conducted on a permissionless network and others on a permissioned network.

As designed and implemented today, DeFi use cases and many DApps use permissionless blockchain networks, such as Ethereum, as the underlying blockchain network. This will likely require significantly different risk and management frameworks if FICUs wish to engage with DeFi innovations. NCUA should examine the development of a methodology for FICUs to evaluate DLT and DeFi DApps. A methodology can be the starting guide to determine what possible risks and compliance measures should be considered by FICUs when evaluating DeFi DApps for possible use internally and offerings to members.

> ***NCUA should examine the development of a methodology for FICUs to evaluate DLT and DeFi DApps.***

11. What unique or specific risks are challenging to measure, monitor, and control for various DLT and DeFi applications? What unique controls or processes are or could be implemented to address such risks?

FICUs participation in blockchain and/or DLT networks will give rise to new risks and challenges. Furthermore, engaging with DeFi DApps present additional possible risks on top of the supporting blockchain or DLT network.

Depending on what type of blockchain and/or DLT network FICUs are participating in, different technologies and processes will be required to address the unique risks including node infrastructure, software maintenance, security and custody. NCUA should examine the different types of blockchain and DLT networks being used in the market and what people, processes and technology might be required for addressing unique risks of each network.

NCUA should examine the different types of blockchain and DLT networks being used in the market and what people, processes and technology might be required for addressing unique risks of each network.

Blockchains and other DLT systems produce transactional data in a new format which must be collected and analyzed in an appropriate manner. Furthermore, this transactional data might be challenging to trace through and analyze depending on how the network is designed. FICUs should be developing the necessary IT infrastructure, data pipelines and/or node infrastructure for the respective blockchain and/or DLT networks they participate in or interact with.

Many digital asset and DeFi use cases involve the use of smart contracts. Smart contracts are a new technology which enable the programmability of assets and the development of DApps on blockchain networks. FICUs should have a clear methodology for identifying, understanding, measuring, and monitoring smart contract risks such as contagion and composability.

DeFi DApps present additional complexity when it comes to risk management. In addition to the underlying blockchain, DeFi DApps rely on complex smart contracts to facilitate financial services on-chain. NCUA should examine and deconstruct the smart contract architecture of DeFi DApps to understand development patterns and the data associated with smart contract interactions.

NCUA should examine and deconstruct the smart contract architecture of DeFi DApps to understand development patterns, and the data associated with smart contract interactions.

13. How are FICUs integrating, or how would FICUs integrate, operations related to DLT and DeFi applications with legacy FICU systems?

FICUs could implement software that act as middleware between their enterprise architecture and the target DLT networks and/or DeFi DApps. Multiple architecture patterns exist to enable a secured blockchain middleware, but ultimately, it's the underlying use case and associated requirements what defines the best approach to follow. Two common patterns used today include dedicated blockchain clients or oracles.

Perhaps the most common pattern used today is integrating enterprise legacy systems using a dedicated blockchain client (e.g., Go Ethereum, Open Ethereum, etc.) that is connected to the target DLT network. Using available software development kits (SDKs) to facilitate programmatic access, FICUs can implement their own protocols to retrieve data from legacy systems and generate blockchain transactions. FICUs could either deploy their own client nodes or utilize cloud-based blockchain-as-a-service (BaaS) offerings from a variety of vendors for a more convenient, secured and faster go-to market strategy. It should be noted that there are different types of nodes such as light, full and archive nodes that FICUs can use, depending on the use case requirements and non-functional trade-offs.

Another way to bridge DLT networks and legacy systems is using blockchain oracles infrastructure. An oracle is a technology which delivers data from an off-chain source to an on-chain smart contract. FICUs can use oracles to retrieve, verify and authenticate data from legacy systems and relay it to smart contracts to initiate and/or interact with on-chain services such as DeFi. Similarly, oracles can be used to send information from a smart contract to a legacy system.

An example of how FICUs can leverage oracle services would be to automatically trigger the transfer of funds locked in a DeFi escrow DApp when a member closes on a new home purchase. The transaction details could be available for all parties to audit and verify.

14. Please identify any potential benefits, and any unique risks, of particular DLT and DeFi applications to FICUs and their members.

We focus on the potential benefits and risks of a permissionless blockchain DeFi borrowing and lending DApp for FICUs and their members. These benefits and risks are in no particular order:

Benefit	Explanation
Increasing financial inclusion	Can be used by members at any time with an internet connection and digital wallet.
Reducing costs	Members can transact for minimal costs (depending on gas costs of particular network), regardless of amount being sent.
Increasing transparency	Transactions are publicly auditable and traceable.
Increasing resiliency	Decentralized infrastructure provides high availability of services.
Increasing transaction speed	Transactions can be sent, verified by the network and settled within minutes.
Increasing financial participation	Enables more members to transact, send value and participate in digital financial services.
Increasing consumer options	Provides new financial services choices and drives provider competition.
Strengthening law enforcement	Can be programed to blacklist addresses in the case of law enforcement request.

Figure 3 – Potential DeFi Benefits

Risk	Explanation
Emerging blockchain technology	DeFi is enabled by blockchains which are still a new and evolving technology. FICUs need to understand complex risks around private key infrastructure, node infrastructure, digital wallets and irreversible transactions.
Smart contract exploits	DeFi DApps leverage smart contracts to create financial services on blockchain networks. FICUs need to understand complex smart contract risks such as exploits and upgrades before offering services to members.
Smart contract contagion	Smart contracts are composable, in that one smart contract might interact with many other smart contracts to build a DApp. Smart contract bugs or exploits could result in a contagion across DeFi DApps.
Lack of decentralization	Some DeFi DApps are decentralized in name only (DINOs). Lack of decentralization could result in operational, governance and other risks for DApp users. FICUs should examine which entities have control of the different aspects of a DeFi DApp
Lack of scalability	DeFi DApps are being deployed on multiple blockchains, each with their own transaction throughput and scalability strategy. FICUs need to understand which blockchains and associated DApps can support their members' usage requirements.

Risk	Explanation
Lack of privacy	Transactions conducted on public blockchains are available for anyone to view. While privacy preserving technologies are being developed, FICUs should consider the risk of members' activity being linked to their real-world identity.
Securing private keys	FICUs could be required to facilitate private key custodian services for members to participate in DApps which would require custody infrastructure and accompanying security processes.

Figure 4 – Potential DeFi Risks

15. What impact will DLT and DeFi applications have on FICUs' earnings? How will FICUs ensure they account for any negative impact, such as potential lost interchange income as peer-to-peer transactions grow?

Digital assets present both an opportunity and threat to FICUs. If FICUs do nothing, earnings could be negatively impacted by technology disruptions. If FICU's lean into digital assets and DeFi, additional value could be delivered by the new products and services offered to members and earnings could be positively impacted.

Some of the possible new products and services which could be built around digital assets:

- Wallet Infrastructure
- Custody Services
- Trading Services
- Borrowing/Lending Services
- Staking Services
- On-chain Analytics

If FICU's lean into digital assets and DeFi, additional value could be delivered by the new products and services offered to members and earnings could be positively impacted.

17. What considerations have commenters given to how to maintain continued compliance with State and Federal laws and regulations that may be applicable to various DLT and DeFi applications, including, but not limited to, those governing securities, Bank Secrecy Act (BSA) and anti-money laundering, and consumer protection? Have those obligations, or uncertainty related to potential obligations, impacted commenters DLT and DeFi activities? How do commenters' DLT and DeFi activities address requirements in these areas?

Generally, there are two emerging paths for ensuring compliance with laws and regulations for DLT and DeFi activities: compliance through "closed gardens" and compliance through on-chain methods.

Compliance through closed gardens is commonly used with services that are provided on a closed digital platform which requires the user to provide specific information to log-in and participate. This approach enables service provides to have granular control of users' actions on their platform and place limitations on possible actions. The service providers of these closed platforms can implement compliance requirements as directed by regulations.

Compliance through on-chain methods is commonly used with services which interact with permissionless blockchain networks. Blockchain (on-chain) analytics enables compliance and risk management through analyzing the history of transactions and address activity. Because permissionless blockchains, like Bitcoin and Ethereum, provide a permanent, tamper-proof history of all transactions to all network participants, on-chain analytics enables those interacting with digital assets and DeFi DApps to perform monitoring, analysis and surveillance of transaction activity. Of note, according to Chainalysis, a leading blockchain analytics firm, less than 1% of all transactions were related to illicit activity in 2020.[4]

NCUA should examine how on-chain methods such as blockchain analytics and oracles can be used to maintain continued compliance for DLT and DeFi DApps.

Another emerging on-chain method for compliance with laws and regulations is by using oracles. Oracles (described in question 13) can provide information from regulators which is then automatically executed by the smart contracts in the DApps. NCUA should examine how on-chain methods such as blockchain analytics and oracles can be used to maintain continued compliance for DLT and DeFi DApps.

Likewise, consumer protection can likely be achieved in various manners. Because the digital asset space is evolving at an exponential pace, member education and disclosure provision are some of the key elements to best ensure consumers are aware of the potential risks associated with DLT and DeFi offerings.

Supervision and Activities Questions (#21-22)

21. Are there any unique aspects the NCUA should consider from a supervisory perspective?

Market structure of digital assets and DeFi is significantly different than traditional financial systems. The same asset may trade in multiple venues in multiple jurisdictions with various regulatory standards, as well as being transacted peer to peer or peer to smart contract. This decentralization of market activities could require new supervisory processes and technologies. NCUA should examine the various options for supervision, such as traditional KYC with centralized providers and on-chain methods for DeFi use cases.

On-chain monitoring involves the analysis of transactional data produced by entities using blockchain and/or DLT networks and smart contracts executing applications. Different blockchain and DLT networks may produce vastly different data types depending on network design. For any off-chain transactions, NCUA cannot rely on blockchain analytics and must work with the centralized FICU entity to understand how funds are handled internally and how the FICU is interacting and delivering the respective product or service.

NCUA should examine the various options for supervision, such as traditional KYC with centralized providers and on-chain methods for DeFi use cases.

[4] https://blog.chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets

22. Are there any areas in which the NCUA should clarify or expand existing supervisory guidance to address these activities?

DeFi – NCUA should consider the following actions:

- Engage FICUs to gauge interest in using or offering DeFi products/services
- Examine DeFi as a potential new backend infrastructure for FICUs
- Potentially clarify or expand supervisory guidance to address FICUs' use of DeFi and potential product/service offerings if appropriate

Stablecoins – NCUA should consider the following actions:

- Engage FICUs to gauge interest in using or offering stablecoin products/services
- Examine the different models of stablecoins which are being issued by private entities
- Examine how these stablecoins are used in the market across various use cases
- Potentially clarify or expand supervisory guidance related to FICUs' stablecoin activity and potential product/service offerings if appropriate

Custody – NCUA should consider the following actions:

- Engage FICUs to gauge interest in using or offering custody services
- Examine the multiple custody models that exist for enabling asset owners to interact with their digital assets and DeFi DApps
- Examine the best practices of custodial risk management frameworks for the different models of custody under different use cases
- Investigate how digital asset custodians segregate individual account funds across different blockchain networks
- Potentially clarify or expand supervisory guidance to address FICUs' custody offerings if appropriate

Share Insurance and Resolution Questions (#24-25)

24. Are there any steps the NCUA should consider to ensure FICU members can distinguish between uninsured digital asset products and insured shares?

Digital asset products complexity and marketing could make it difficult for customers to clearly distinguish between uninsured products and insured shares. There are multiple methods which could be used to help customers distinguish between the different types of products and insured shares; directly on-chain and off-chain via financial institution disclosures, account structuring or other tagging mechanisms.

Prioritizing member education and increasing financial literacy around digital asset and DeFi products/services is critical. An example of increasing member education could be to require members complete a learning module on a specific DeFi product before they can engage with it. NCUA should consider the different methods FICUs can take to help members distinguish between traditional assets and digital asset products.

Prioritizing member education and increasing financial literacy around digital asset and DeFi products/services is critical.

25. Are there distinctions or similarities between stablecoins (cryptocurrencies that are backed by a currency like the U.S. Dollar and are designed to have a stable value compared to other cryptocurrencies) and stored value products where the underlying funds are held at FICUs and, for which pass-through share insurance may be available to members in limited scenarios?

Certain fiat-backed stablecoins might have similarities to stored value products in that one can purchase stablecoins, hold them in a digital wallet and transact with them for different products/services. Because there are various models for fiat-backed stablecoins, the NCUA should examine the various fiat-backed stablecoin models and potentially produce guidance regarding underlying collateral transparency, usage and proof of reserves.

Additional Considerations

We applaud the NCUA for establishing the Office for Financial Technology and Access. We recommend further empowerment and elevation of the Office to coordinate NCUA's oversight and response to digital asset and DeFi activities. Other U.S financial regulators such as the SEC, with FinHub, and CFTC, with LabCFTC, have successfully empowered and elevated the fintech entities within their agencies. These fintech-focused entities enable the agencies to keep pace with industry developments and engage with innovators to understand the nuances of new products and services at a granular level. NCUA could consider collaborating with these other fintech offices across agencies to share knowledge and harmonize regulations.